REMARKS:

In the Office Action the Examiner noted that claims 1-17 are pending in the application, and the Examiner rejected all claims. Claims 1, 6-8 and 13-15 are amended herein. New claims 18 and 19 are added, and claims 4, 11, 16 and 17 are cancelled without prejudice. No new matter is presented. Support for the amendments can be found at least on page 9 line 5 through page 13 line 8, and Figs. 1 to 3.

Thus, claims 1-3, 5-10, 12-15, 18 and 19 are pending and under consideration. The rejections are traversed below.

REJECTION UNDER 35 U.S.C. § 103(a):

In item 3 on page 2 of the Office Action the Examiner rejected claims 1-4, 6-11, 13-15, 16, and 17 under 35 U.S.C. § 103(a) as being unpatentable over Design of Conventional Cryptographic Algorithms reference by Preneel et al. (Preneel) in view of U.S. Patent No. 6,501,840 (Saijo).

Claims 5 and 12 were rejected under 35 U.S.C. §103(a) as being unpatentable over Preneel in view of Saijo and further in view of U.S. Patent No. 6,182,216 (Luyster).

Preneel does not teach or suggest "tentatively deciding, combining and determining until a number of the combined integer numbers becomes equal to a final number that is calculated based on the memory capacity and the entire inputting and outputting bit number" and "selecting, when the number of the combined integer numbers becomes equal to the final number, the combined integers of the third set to be an optimal combination of input and output bit numbers of each of the S-box", as recited in claim 1. Claims 8 and 15 also recite similar features.

The invention of claim 1 includes "dividing the entire input and output bit number by the initial value to acquire an integer quotient and an integer remainder" and "making a first set composed of the integer quotient pieces of the initial value", acquiring "a second set" and "combining the integer numbers so as to make a third set of integer composed of combined integers." See also claims 8 and 15.

Instead, Preneel discusses S-boxes where 8 input bits are transformed into 32 or 64 output bits and value of S-boxes is selected at random or to achieve certain properties of an encryption standard (i.e., DES) (see, page 113, paragraph 3 in section 4.2). Meaning, Preneel is restricted to selecting a value for the S-boxes at random or in accordance with encryption

standard used.

As discussed above, claims 1, 8 and 15 patentably distinguish over Preneel. Further, as Saijo does not optimize input and output data for each block because the input data size, upon which the output data size depends, is extracted from input data/message to be sent, Saijo does not cure the deficiencies of Preneel regarding the independent claims of the present application.

In particular, Saijo is limited to calculating the input and the output bits based on a preset size of the data being transferred from a cryptographic processing unit.

On the other hand, Luyster divides the input block into data segments using minimum size of round segments (see, col. 16, lines 59-64), where the block size is not variable and the minimum size of the round segments rotated by a data dependent variable is limited to at least 32 bits.

The cited references, alone or in combination, do not teach or suggest the above-identified features including "tentatively deciding", "combining" and "selecting", as recited in the independent claims (see above discussion of claims).

Claims depending from the independent claims include all of the features of that claim plus additional features which are not disclosed by the cited references. The dependent claims are also independently patentable. For example, the invention of claim 3 "selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device". The cited references do not teach or suggest this feature of claim 3.

At least on page 6 of the outstanding Office Action, the Examiner asserts that it would be obvious to one of ordinary skill in the art to combine the teachings of Luyster and Preneel-Saijo because it is well known in the art that the size affects the efficiency and security of a cryptographic process and a minimum bound is required to maintain satisfactory performance. Applicants respectfully traverse the Examiner's statement.

Specifically, Applicants submit that no supporting evidence related to the claimed "selecting" including specifying "a smallest value of the input and output number of said plurality of S-boxes" as recited in claims 5 and 12 has not been provided, and request that the Examiner produce authority for the statement.

Even assuming the Examiner's well known rejection is appropriate, the invention of

claims 5 and 12 is patentably distinguishable over the cited references for at least the reasons mentioned above with respect to claims 1 and 8, upon which claims 5 and 12 depend.

Therefore, withdrawal of the rejection is respectfully requested.

CONCLUSION:

There being no further outstanding objections or rejections, it is respectfully submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 10/23/2007

By: Temnit Afework

Temnit Afework
Registration No. 58,202

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501